REMARKS

Claims 1-19 are all the claims pending in the application.

Applicants note that a number of editorial amendments have been made to the specification to improve the form thereof. No new matter has been added.

Applicants also note that a number of non-narrowing editorial changes have been made to the claims to place the claims in better U.S. form. Such changes have not been made in response to any prior art rejection or other rejection.

I. Claim Rejections under 35 U.S.C. § 103(a)

Claims 1-19 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Goss (U.S. 4,956,863). Applicant respectfully traverses this rejection on the following basis.

Claim 1 recites that at least the random number generator and the public key generator are formed on one semiconductor integrated circuit; claim 5 recites that at least the random number generator and the shared key generator are formed on one semiconductor integrated circuit; claim 9 recites that at least the random number generator, the public key generator, and the shared key generator are formed on one semiconductor integrated circuit; and claim 13 recites that at least the random number generator, the secret key holding unit, the public key generator, and the shared key generator are formed on one semiconductor integrated circuit..

Regarding the above-noted features, the Examiner has recognized in the Office Action that Goss does not teach or suggest such features (see Office Action at page 4). The Examiner, however, has taken the position that it would have been obvious to form the random number generator, the secret key holding unit, the public key generator, and the shared key generator of

Goss on one semiconductor circuit because "the method of Goss has been known in the art for almost two decades, and one of ordinary skill in the art would be able to implement this method on one semiconductor chip." Applicant respectfully disagrees with the Examiner's position.

Initially, Applicant submits that the Examiner has merely set forth a conclusory statement of obviousness without providing any explanation as to why one of ordinary skill in the art would have made such a modification to Goss.

In this regard, as explained in MPEP 2141(III), Applicant notes that the Examiner is required to "explain why the difference(s) between the prior art and the claimed invention would have been obvious to one of ordinary skill in the art" (emphasis added). In addition, the MPEP also explains that "[r]ejections on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness" (see MPEP 2141(III)).

Based on the foregoing, Applicant respectfully submits that the Examiner's conclusory statement that "the method of Goss has been known in the art for almost two decades, and one of ordinary skill in the art would be able to implement this method on one semiconductor integrated circuit" does not constitute a prima facie case of obviousness.

Further, with respect to the disclosure of Goss, Applicant notes that while this reference discloses the ability to add a signature to a key in the case that the communication channel 26 is being eavesdropped (see Fig. 3), that Goss does not disclose the ability to prevent the eavesdropping of certain values, algorithms and variables, such as a value of Xa', a value of "signed Ya", an algorithm performed by key generator 18, a digital signature algorithm, and variables α and p.

In this regard, Applicant notes that the above-noted values, algorithms, and variables are elements that constitute a basis of a public key cryptosystem, and when such elements are attacked and information is leaked, the information on the communication channel 26 of Goss may be easily stolen. In this regard, Applicant notes that in Fig. 5 of Goss, which depicts the cryptographic processor 60, it would be easy to observe the contents of RAM 68, ROM 70, data bus 64, and address bus 66, and thus, the above-noted algorithms could be easily stolen.

In contrast, as explained in connection with the present invention, by forming the elements identified above in claims 1, 5, 9 and 13 on one semiconductor integrated circuit, and controlling such elements by a controller, it is possible to prevent the above-noted algorithms from being stolen.

In view of the foregoing, Applicant respectfully submits that it would not have been obvious to one of ordinary skill in the art to modify Goss so as to provide each of the above-noted features recited in claims 1, 5, 9 and 13. Accordingly, Applicant submits that claims 1, 5, 9 and 13 are patentable over Goss, an indication of which is kindly requested.

Claims 2-4 depend from claim 1; claims 6-8 depend from claim 5; claims 10-12 and 18 depend from claim 9; and claims 14-17 and 19 depend from claim 13. Accordingly, Applicant submits that these claims are patentable at least by virtue of their dependency.

II. Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited.

If any points remain in issue which the Examiner feels may best be resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Ryogo YANAGISAWA

By: Kenneth W. Fields

Kenneth W. Fields
Registration No. 52,430
Attorney for Applicant

KWF/ra
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
November 19, 2007